Blueprint for Information Sharing

Locking the Backdoor to America's Information Systems Infrastructure

The Initiative for State Infrastructure Protection (ISIP)

Critical infrastructures—such as transportation and energy—are typically owned by private industry and regulated by state governments. They provide services that sustain public health and the economy. The computer—"cyber"—systems that control the operations of these infrastructures are vulnerable to attacks. The threats include computer hackers "breaking-in", computer viruses hidden in software and other deceptive ways of exploiting computer vulnerabilities. These attacks can lead to disruption or catastrophic loss of key services. It is in the best interest of a state to secure these vulnerabilities, ensuring continuity of public services.

The Initiative for State Infrastructure Protection (ISIP) is a Department of Defense (DoD) program from which state and local governments can have access to a proven and extensive knowledge base to support their cyber security efforts. The National Guard is an asset in each state, under the authority of each governor. It is the primary interface between a state government and the ISIP program. Each state National Guard has a Computer Emergency Response Team (CERT). The capabilities of the CERTs constitute a resource that state governments can use to protect the information systems that control critical infrastructures, such as transportation, energy, etc.

The defense of the United States, in peacetime and wartime, requires the ability to mobilize at a moment's notice. Mobilization depends on transportation, energy and other resources that are owned by private industries and regulated by state governments. Sharing information that improves the security of critical infrastructures is in the interest of the DoD.

Through the ISIP program, state planners can take advantage of successful coordination, access current information, and learn from their peers through sharing relevant experiences. An important access point to ISIP, is through the website (www.army.mil/ciog6/isip). This site contains a wealth of information plus the experience and best practices of participating organizations. It promotes proactive security activities instead of simply responding to threats. Participants are asked to share their experiences and best practices with their peers, but there is no formal commitment necessary to take advantage of the program.

The ISIP program is a unique government resource that promotes the sharing of knowledge. The threat of cyber attack is real and this threat will not diminish in the foreseeable future. Programs, such as ISIP, that support the creation and implementation of

effective, efficient local cyber security will strengthen our technology advantage and help secure our national infrastructure.

A state with an interest in protecting its critical infrastructures should address several questions:

⊕ **Have you assessed and documented your critical infrastructures?**

In order to identify and understand which infrastructures are vulnerable, a state should document the specific configurations of hardware and software that interface with a particular infrastructure. Once these configurations are identified, then relevant cyber security measures can be implemented.

A key component of the ISIP program is dissemination of timely, accurate vulnerability information concerning cyber systems. The information is shaped into the Information Assurance Vulnerability Alert (IAVA). Each IAVA identifies the vulnerable systems and software, assesses the vulnerability and provides solutions to mitigate or prevent exploitation. Currently, the IAVAs and related DoD information flows to the National Guard CERTs. ISIP is facilitating a process to share that same information with state chief information officers and/or "state infrastructure protection centers" (SIPC).

A state can benefit greatly by developing its own SIPC. Several states—including Arizona and Texas—have SIPCs that serve as a coordinated nexus of cyber security information.

⊕ **Do you have a coordinated, centralized process for sharing critical vulnerability attack information?**

The ability of a state government to effectively disseminate critical cyber vulnerability information is dependant on a coordinated and centralized process. Several states have created state infrastructure protection centers (SIPC) to fulfill this objective. The SIPC coordinates with state and federal resources in the National Guard, law enforcement, emergency services and private sector organizations that own and operate critical infrastructures. They establish standard operating procedures (SOP) and two-way lines of communication with state and federal agencies.

⊕ **Do you have cyber security training for government IT officials?**

The cyber security of critical infrastructures also requires awareness, training, education and experience. The basic level is general awareness generic concepts and terms that apply to any cyber system that interfaces with an infrastructure. It is the point-of-entry into the progression of cyber security training. The private and public sectors, at both the federal and state levels have information security awareness, training and education programs. Some of the best sources are private organizations that also conduct conferences. An good example is the DoD. It has streamlined training into tiers and key functional areas. Training, education and experience build upon awareness with increasing detail and direct application. This whole process should be extensible, by allowing for advances in technology.

⊕ **Do you conduct exercises to test your cyber security?**

Practical simulations and exercises are important aspects to understanding vulnerabilities of a particular information system. Exercises take one of three forms: tabletop, functional and field training. Tabletop is the least expensive, involving key personnel in a scripted scenario. A functional training exercise involves only a discrete operational function of a network. Field training exercises are the most intensive in time and money, involving the entire network or large segment of the network. The National Guard, CERTs conduct functional training exercises on a regular basis. An example is a "capture-the-flag" where the CERT divides into attacking and defensive teams in a closed, laboratory environment.